IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Graeme John Proudler		
Assignee:	Hewlett-Packard Development Company L.P.		
Title:	Method and Apparatus for Managing a Hierarchy of Nodes		
Serial No.:	10/688,397	Conf. No.	1309
Examiner:	Randal Moran	Group Art Unit:	2435
Docket No.:	200309650-3	Filing Date:	October 16, 2003

April 17, 2009

Mail Stop APPEAL BRIEF-PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Dear Sir:

This submission, which is in reply to the Notification of Non-Compliant Appeal Brief dated April 1, 2009 and to the Office Communication dated March 20, 2009 in the above-identified patent application, is being submitted within one month of the date of the Notification of Non-Compliant Appeal Brief (i.e., before May 1, 2009).

Appellant requests consideration of the Appeal Brief as supplemented by the following "SUMMARY OF CLAIMED SUBJECT MATTER."

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

SUMMARY OF CLAIMED SUBJECT MATTER

The present application relates to managing a hierarchy of keys that a trusted computing platform uses for the protection of sensitive data. More specifically, a trusted computing platform can employ a tree-structured key hierarchy having non-leaf nodes, each of which is associated with an encrypted form of a key used to encrypt any keys associated with its child nodes or node. (The leaf nodes need not be keys.) Such a tree structure is used to provide "protected storage" for a trusted platform according to TCG specifications (TCG is the Trusted Computing Group which is the successor to the TCPA group mentioned in the specification). A root key of the key hierarchy is called the "storage root key" or "SRK" in the present application and is held in decrypted form in secure storage of a "trusted platform module" or TPM. The rest of the tree structure is encrypted and thus can be stored in normal memory. The claimed invention concerns replacing the storage root key (SRK) with a descendant key from the hierarchy (such a key is called a dynamic root key or DRK in the specification); in this state, only those hierarchy nodes descendant from the current dynamic root key currently can be accessed. Those parts of the hierarchy that could only be reached by descent from the original storage root node, and not via the dynamic root key, become inaccessible.

Independent claim 35 is specifically directed to a computing platform including a secure key-handling unit and insecure storage. In an embodiment of the invention illustrated in Fig. 3, the recited secure key handling unit and insecure memory respectively correspond to Trusted Platform Module (TPM) 10 and normal memory 22. Secure key-handling unit 10 stores a storage root key 11 that forms the root node of a tree-structured node hierarchy such as illustrated by nodes K1-1 … shown in Fig. 1 or 3 and described in the specification beginning at page 6, line 32. Other than the root node, each non-leaf node has, in encrypted form, a key used to encrypt each of its child nodes. (See page 7, lines 2-3.) The insecure storage stores the hierarchy nodes K1-1…K2-1… other than the root node (e.g., other than SRK 11). Claim 35 further recites, the key-handling unit includes, "a memory for storing a current decryption-root key." The memory corresponds to storage of the TPM 10 described at page 7, lines 1-2 and storing a current root key or DKR is described at page 11, lines 1-3. The key-handling unit further includes, "a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes decryptable by a chain of decryption rooted in said current decryption-root key." See page 4, line 31 to page 5, line 3. The final

PATENT LAW OFFICE OF
DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

recited element of the key handling unit is "a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed." See, for example, page 10, lines 5-8 and page 11, lines 1-8.

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

REMARKS

The Notification of Non-Compliant Appeal Brief dated April 1, 2009 indicated that the Appeal Brief submitted February 4, 2008 in the above-identified patent application failed to provide a summary of the claimed subject matter as required by 37 CFR 41.37(c)(1)(v). In particular, the Notification indicated that the Appeal Brief did not refer to independent claim 35 with reference to the specification page and line numbers or to the drawings. Pursuant to MPEP 1205.03, Appellant is providing the above Summary of the Claimed Subject Matter, which includes additional references to Appellant's specification and drawings. The new Summary of the Claimed Subject Matter is intended to replace the section having the same title in the Appeal Brief filed February 4, 2008.

The fee required under 37 CFR 41.20(b)(2) for filing of the Appeal Brief was previously paid. Accordingly, Applicant believes that no further fee is required. However, the Commissioner is authorized to charge Deposit Account No. 08-2025 any fee which may be required for consideration of the Appeal Brief as modified herein.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this document.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543